

BEST AVAILABLE COPY

**Amendment and Response**

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1/H300.126.101

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES**REMARKS**

The following remarks are made in response to the Office Action mailed January 13, 2006. Claims 1-28 were rejected. With this Response, claims 1 and 13 have been amended. Claims 1-28 remain pending in the application and are presented for reconsideration and allowance.

**Claim Objections**

The Examiner objected to the amended claims filed on October 28, 2005 having the same notation as the claims filed on July 22, 2005. Applicant respectfully notes that future responses to actions will only mark newly amended claims with the underlining and strike through notation. Applicant respectfully notes that the amendment filed on July 22, 2005 was not considered by the Examiner in the non-final Office Action mailed July 28, 2005. Therefore, in responding to the July 28, 2005 non-final Office Action, Applicant assumed that the October 28, 2005 amendment and response needed to include the amendments submitted with the amendment and response filed July 22, 2005. Applicant apologizes for any inconvenience.

**Claim Rejections under 35 U.S.C. § 112**

The Examiner rejected claims 1-28 under 35 § U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner rejected claims 1-28 because the term "PKI" is stated in the claims along with unsigned documents. The Examiner states that "it is inherent in a PKI system that the certificate, or ticket is signed. It is part of the definition Newton's Telecom Dictionary '... procedures for the distribution of public keys via digital certificates signed by Certificate Authorities ...'"

Applicant respectfully submits that it is not inherent in a PKI system that the certificate or ticket is signed. For example, the general definition provided by the Newton's Telecom Dictionary provides that a PKI is "a means by which public keys can be managed on a secure basis for use by widely distributed users or systems." This general definition corresponds to the meaning of PKI in the claims and in the present specification. The text of

**Amendment and Response**

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1/H300.126.101

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES

the Newton's Telecom Dictionary definition cited by the Examiner is actually specifically directed to an example standard referred to as the X.509 Standard and specifically states that the "X.509 Standard is widely accepted as the basis for such an infrastructure. X.509 defines data formats, key infrastructure components (e.g., security administrators, certificate authorities, users, and directories), and procedures for the distribution of public keys via digital certificates signed by Certificate Authorities (CAs)." Thus, the language cited by the Examiner is not directed to PKIs in general but specifically to the X.509 Standard, which does not need to be implemented in every PKI. For example, the Newton Telecom Dictionary defines public key encryption (PKE) and provides a general definition but also cites certain standards and encryption schemes, such as pretty good privacy (PGP) and RSA data security, even though PGP and RSA data security do not need to be used for public key encryption. Moreover, as to the specific X.509 Standard cited in the Newton's Telecom Dictionary, standards can change with updated versions and can be replaced by other standards. In addition, even though the X.509 certificate normally includes a digital signature from a certificate authority, the most common commercial variety of a root certificate, which is an unsigned public key certificate, is based on the X.509 Standard. See Root Certificate from Wikipedia, the free encyclopedia <[http://en.wikipedia.org/wiki/root\\_certificate](http://en.wikipedia.org/wiki/root_certificate).

Thus, Applicant respectfully submits that the public key infrastructure (PKI) as defined in the limitations of claims 1-28 and also defined in the present specification corresponds to the general definition provided in the Newton's Telecom Dictionary of a means by which public keys can be managed on a secure basis for use by widely distributed users or systems. The invention defined by claims 1-28 relates to a PKI which manages public keys on a secure basis for use by widely distributed users or systems which uses certificates which are issued by a certificate authority but not signed by the certificate authority.

The Examiner rejected claims 1-28 because in a comprising claim, such as claims 1 and 13, it is not clear how the limitation of "not signed" effects the remaining portions of the claim.

Applicant has amended independent claims 1 and 13 to further clarify the claim language to now include that the issued certificates are not signed by the certificate authority and are valid until at least one of revoked by the certificate authority and expired. Thus,

**Amendment and Response**

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1/H300.126.101

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES

amended independent claims 1 and 13 include limitations of a certificate authority issuing a first certificate to a subject, the certificate including a public key of the subject, long-term identification information related to the subject, and meta-data related to the first certificate, wherein the first certificate is not signed by the certificate authority. The certificate authority maintains a database of records representing issued certificates in which it stores a record representing the first certificate, wherein the issued certificates are not signed by the certificate authority and are valid until at least one of revoked by the certificate authority and expired. A verifier maintains a hash table containing cryptographic hashes of valid certificates corresponding to the records stored in the database and including a cryptographic hash of the first certificate.

By contrast, conventional public key cryptography systems, such as the public key cryptography system disclosed in the Stallings "How to Protect the Company Jewels" reference, typically provide that the certificate authority issue signed certificates and the recipient of the signed certificate calculate the hash code of the unsigned certificate and compare this to the hash code recovered from the signed certificate. If the two codes match, this is a valid certificate and the recipient may trust the public key in that the signed certificate belongs to the identified user. Whereas defined by amended independent claims 1 and 13, the certificate authority issues certificates that are not signed by the certificate authority and are valid until at least one of revoked by the certificate authority and expired, the certificate authority maintains a database of records representing issued certificates, and the verifier maintains a hash table containing certificate of hashes of valid certificates corresponding to the records stored in the database and includes a cryptographic hash of the first certificate, wherein the subject presents the issued first certificate to the verifier for authentication and demonstrates that the subject has knowledge of a private key corresponding to the public key of the first certificate. In this way, the invention defined by independent claims 1 and 13 permits a means by which public keys can be managed on a secure basis for use by widely distributed users or systems without the expensive need for the certificate authority signing the certificate. Thus, amended independent claims 1 and 13 now clearly define how issued certificates are not signed by the certificate authority and are valid until at least one of revoked by the certificate authority and expired and the claims include

**Amendment and Response**

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1/H300.126.101

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES

further limitations to permit a PKI to operate properly without the normal expensive mechanism of having a certificate authority issue a signed certificate.

In view of the above, claims 1-28 are believed to be in form for allowance.

Therefore, Applicant respectfully requests that rejections to these claims under 35 U.S.C. § 112, second paragraph, be reconsidered, and that the rejections be removed and these claims be allowed.

**Claim Rejections under 35 U.S.C. § 103**

The Examiner rejected claims 1, 2, 6, 7, 8, 13, 14, 18, 19, 20, 25, and 26 under 35 U.S.C. § 103(a) as being unpatentable over the Stallings "How to Protect the Company Jewels" reference in view of the Fischer U.S. Patent No. 5,475,826.

The Examiner rejected claims 3, 4, 15, and 16 under 35 U.S.C. § 103(a) as being unpatentable over the Stallings "How to Protect the Company Jewels" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of the Maruyama et al. U.S. Patent No. 6,393,563.

The Examiner rejected claims 5 and 17 under 35 U.S.C. § 103(a) as being unpatentable over the Stallings "How to Protect the Company Jewels" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of the Kausik et al. U.S. Patent No. 6,263,446.

The Examiner rejected claims 9, 21, 27, and 28 under 35 U.S.C. § 103(a) as being unpatentable over the Stallings "How to Protect the Company Jewels" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of the Gasser et al. U.S. Patent No. 5,224,163.

The Examiner rejected claims 10 and 22 under 35 U.S.C. § 103(a) as being unpatentable over the Stallings "How to Protect the Company Jewels" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of Micali U.S. Patent No. 5,793,868 in view of the Boyle et al. U.S. Patent No. 6,212,636.

The Examiner rejected claims 11 and 23 under 35 U.S.C. § 103(a) as being unpatentable over the Stallings "How to Protect the Company Jewels" reference in view of the Fischer U.S. Patent No. 5,475,826 in view of the Micali U.S. Patent 5,793,868 in view of the Perlman et al. U.S. Patent No. 5,687,235.

The Examiner rejected claims 12 and 24 under 35 U.S.C. 103(a) as being unpatentable over the Stallings "How to Protect the Company Jewels" reference in view of

**Amendment and Response**

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1/H300.126.101

Title: **LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES**

the Fischer U.S. Patent No. 5,475,826 in view of the Micali U.S. Patent No. 5,793,868 in view of the Boyle et al. U.S. Patent No. 6,212,636 in view of the Gasser et al. U.S. Patent No. 5,224,163.

Independent claims 1 and 13 are not taught or suggested by the combination of the Stallings reference and the Fischer patent. The Examiner admits that the Stallings reference does not teach a verifier maintaining cryptographic hashes. The Examiner cites the Fischer patent which teaches maintaining hashes of files in a security database.

Amended independent claims 1 and 13 includes limitations of a certificate authority issuing a first certificate to a subject, the first certificate including a public key of the subject, long-term identification information related to the subject, and meta-data related to the first certificate, wherein the first certificate is not signed by the certificate authority. The certificate authority maintains a database of records representing issued certificates in which it stores a record representing the first certificate, wherein the issued certificates are not signed by the certificate authority and are valid until at least one of revoked by the certificate authority and expired. Amended independent claims 1 and 13 further recite that a verifier maintains a hash table containing cryptographic hashes of valid certificates corresponding to the records stored in the database and including a cryptographic hash of the first certificate.

Neither the Stallings reference nor the Fischer patent teach or suggest a verifier maintaining a hash table containing cryptographic hashes of valid certificates wherein issued certificates are not signed by the certificate authority and are valid until at least one of revoked by the certificate authority and expired, wherein the hash table includes a cryptographic hash of the first certificate having a public key of the subject, long-term identification information related to the subject, and meta-data related to the first certificate, wherein the first certificate is not signed by the certificate authority as recited in amended independent claims 1 and 13. As admitted by the Examiner, the Stallings reference does not teach a verifier maintaining cryptographic hashes, furthermore, the Fischer patent teaches a system that maintains hashes of files in a security database not a verifier maintaining a hash table containing cryptographic hashes of valid certificates, wherein issued certificates are not signed by the certificate authority and are valid until at least one of revoked by the certificate authority and expired and the hash table includes a cryptographic hash of the first certificate including a public key of the subject, long-term identification information related to the

**Amendment and Response**

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1/H300.126.101

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES

subject, and meta-data related to the first certificate, wherein the first certificate is not signed by the certificate authority.

In addition, the Stallings reference does not teach or suggest a certificate authority issuing unsigned certificates. The Stallings reference discloses a certificate authority (CA) that creates unsigned certificates and then takes the hash code of this unsigned certificate. Next, the CA encrypts the hash code with the CA's private key to produce a signature. The CA attaches the signature to the certificate to form the signed certificate which is issued such that the user may supply the certificate to any one who needs the user's public key. To verify that a public key is valid, the recipient recovers the hash code from the signature by decrypting the signature using the CA's public key. Then, the recipient calculates the hash code of the unsigned certificate and compares this to the hash code recovered from the signature in the signed certificate. If the two codes match, this is a valid certificate and the recipient may trust that the public key in that signed certificate belongs to the identified user. Thus, the CA disclosed in the Stallings reference creates unsigned certificates but issues signed certificates so that the recipient can use the signed certificate to assure a valid certificate and that the recipient may trust that the public key in the signed certificate belongs to the identified user. Thus, the Stallings reference does not teach or suggest issuing certificates that are not signed by the certificate authority.

In view of the above, amended independent claims 1 and 13 are not taught or suggested by the combination of the Stallings reference and the Fischer patent. As dependent claims 2-12 and 25-27 further define patentably distinct amended independent claim 1; and as dependent claims 14-24 and 28 further define patentably distinct amended independent claim 13, these dependent claims are also believed to be allowable.

Therefore, Applicant respectfully requests reconsideration and withdrawal of the 35 U.S.C. § 103 rejections to claims 1-28 and allowance of these claims.

**CONCLUSION**

In view of the above, Applicant respectfully submits that pending claims 1-28 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-28 is respectfully requested.

**Amendment and Response**

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1/H300.126.101

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES

No fees are required under 37 C.F.R. 1.16(h)(i). However, if such fees are required, the Patent Office is hereby authorized to charge Deposit Account No. 08-2025.

The Examiner is invited to contact the Applicant's representative at the below-listed telephone numbers to facilitate prosecution of this application.

Any inquiry regarding this Amendment and Response should be directed to either Patrick G. Billig at Telephone No. (612) 573-2003, Facsimile No. (612) 573-2005 or Kevin Hart at Telephone No. (970) 898-7057, Facsimile No. (970) 898-7247. In addition, all correspondence should continue to be directed to the following address:

IP Administration  
Legal Department, M/S 35  
HEWLETT-PACKARD COMPANY  
P.O. Box 272400  
Fort Collins, Colorado 80527-2400

Respectfully submitted,

Francisco Corella,

By his attorneys,

DICKE, BILLIG &amp; CZAJA, PLLC

Fifth Street Towers, Suite 2250

100 South Fifth Street

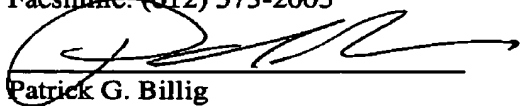
Minneapolis, MN 55402

Telephone: (612) 573-2003

Facsimile: (612) 573-2005

Date: April 13, 2006

PGB:mlm

  
Patrick G. Billig  
Reg. No. 38,080**CERTIFICATE UNDER 37 C.F.R. 1.8:**

The undersigned hereby certifies that this paper or papers, as described herein, are being transmitted via facsimile to Facsimile No. (571) 273-8300 on this 13 day of April, 2006.

By: 

Name: Patrick G. Billig

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☒ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**